

72
J1033 U.S. PTO
09/836222
04/18/01

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Yoshihiro NAKAGAWA

Group Art Unit: To Be Assigned

Serial No.: To Be Assigned

Examiner: To Be Assigned

Filed: April 18, 2001

For: INDIVIDUAL INFORMATION MANAGING DEVICE

**SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN
APPLICATION IN ACCORDANCE
WITH THE REQUIREMENTS OF 37 C.F.R. § 1.55**

*Assistant Commissioner for Patents
Washington, D.C. 20231*

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, Applicants submit herewith a certified copy of the following foreign application:

Japanese Patent Application No. 2000-397492 filed December 27, 2000.

It is respectfully requested that Applicants be given the benefit of the foreign filing date, as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. § 119.

Respectfully submitted,

STAAS & HALSEY LLP

Dated: April 18, 2001

By:



James D. Halsey, Jr.
Registration No. 22,729

700 Eleventh Street, N.W.
Suite 500
Washington, D.C. 20001
(202) 434-1500

IN THE U.S. PATENT AND TRADEMARK OFFICE

Applicant(s): SUMIDA, Yoshiaki

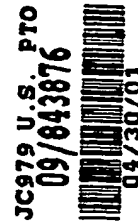
Application No.:

Group:

Filed: April 30, 2001

Examiner:

For: WIRELESS SEARCH DEVICE



LETTER

Assistant Commissioner for Patents
Box Patent Application
Washington, D.C. 20231

April 30, 2001
1152-0276P

Sir:

Under the provisions of 35 USC 119 and 37 CFR 1.55(a), the applicant hereby claims the right of priority based on the following application(s):

<u>Country</u>	<u>Application No.</u>	<u>Filed</u>
JAPAN	2000-228905	07/28/00

A certified copy of the above-noted application(s) is(are) attached hereto.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to deposit Account No. 02-2448 for any additional fees required under 37 C.F.R. 1.16 or under 37 C.F.R. 1.17; particularly, extension of time fees.

Respectfully submitted,

BIRCH, STEWART, NOLASCH & BIRCH, LLP

By:


CHARLES GORENSTEIN

Reg. No. 29,271

P. O. Box 747

Falls Church, Virginia 22040-0747

Attachment
(703) 205-8000
/pf

日本国特許庁

PATENT OFFICE
JAPANESE GOVERNMENT

J1033 U.S. PTO
09/836222
04/18/01

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日

Date of Application:

2000年12月27日

出願番号

Application Number:

特願2000-397492

出願人

Applicant(s):

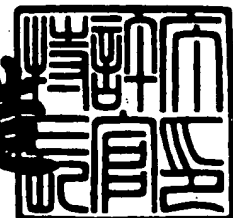
富士通株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2001年 3月16日

特許庁長官
Commissioner,
Patent Office

及川耕造



出証番号 出証特2001-3019419

【書類名】 特許願

【整理番号】 0090210

【提出日】 平成12年12月27日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 15/00

【発明の名称】 個人情報管理装置

【請求項の数】 7

【発明者】

 【住所又は居所】 香川県高松市錦町1丁目11番1号 株式会社富士通四
 国インフォテック内

 【氏名】 中川 喜博

【特許出願人】

 【識別番号】 000005223

 【氏名又は名称】 富士通株式会社

【代理人】

 【識別番号】 100094330

 【弁理士】

 【氏名又は名称】 山田 正紀

【選任した代理人】

 【識別番号】 100109689

 【弁理士】

 【氏名又は名称】 三上 結

【手数料の表示】

 【予納台帳番号】 017961

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

 【物件名】 図面 1

 【物件名】 要約書 1

特 2 0 0 0 - 3 9 7 4 9 2

【包括委任状番号】 9912909

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 個人情報管理装置

【特許請求の範囲】

【請求項 1】 通信回線網に接続された、個人情報を管理する個人情報管理装置であって、

個人ごとの情報が登録された個人情報格納部と、

各個人により指定された各個人ごとの情報開示手続が登録された開示手続格納部と、

通信回線網を経由した、特定の個人の情報の開示依頼を受け、前記開示手続格納部に格納された、該特定の個人の情報開示手続に合致した情報開示手続を実行し、該情報開示手続が満足された場合に該特定の個人の情報を依頼元に向けて通信回線網に送信する開示手続実行部とを備えたことを特徴とする個人情報管理装置。

【請求項 2】 前記個人情報格納部は、個人ごとの情報の中の各個別の情報それぞれが各個人により複数のランクのうちのいずれかのランクに指定されることにより、各個人内で複数にランク付けされてなる個人情報が登録されたものであり、

前記開示手続格納部は、各個人により指定された、各個人内の各ランクに応じた情報開示手続が登録されたものであって、

前記開示手続実行部は、特定の個人の情報の開示依頼を受け、前記開示手続格納部に格納された、該特定の個人の、開示依頼を受けた情報のランクに応じた情報開示手続に合致した情報開示手続を実行するものであることを特徴とする請求項 1 記載の個人情報管理装置。

【請求項 3】 前記開示手続格納部は、各個人により指定された、各個人ごとの平常時の情報開示手続に加え、各個人により指定された、各個人ごとの緊急時の情報開示手続が登録されたものであって、

前記開示手続実行部は、平常時と緊急時とを識別する情報を伴った、特定の個人の情報の開示依頼を受け、該開示依頼が平常時あるいは緊急時のいずれに属するかに応じて、前記開示手続格納部に格納された、該特定の個人の、それぞれ平

常時の情報開示手続あるいは緊急時の情報開示手続に合致した情報開示手続を実行するものであることを特徴とする請求項 1 記載の個人情報管理装置。

【請求項 4】 前記開示手続格納部は、個人ごとの情報開示手続の一部として、各個人により指定された、該各個人への連絡手続が登録されたものであって、

前記開示手続実行部は、特定の個人の情報の開示依頼を受けて、該特定の個人に、前記開示手続格納部に格納された該特定の個人への連絡手続に合致した連絡手続で、個人情報の開示依頼があった旨通知して、通知を受けた個人からの情報開示の承認を受ける開示依頼通知部を備え、該開示依頼通知部により情報開示の承認を受けて、さらに情報開示手続を進めるものであることを特徴とする請求項 1 記載の個人情報管理装置。

【請求項 5】 前記開示手続格納部は、個人ごとの情報開示手続の一部として、各個人により指定された、該各個人本人であることを認証する認証手続が登録されたものであって、

前記開示手続実行部は、特定の個人の情報の開示依頼を受けて、前記開示手続格納部に格納された該特定の個人の認証手続に合致した認証手続で該特定の個人の認証を行なう認証部を備えたものであることを特徴とする請求項 1 記載の個人情報管理装置。

【請求項 6】 前記開示手続格納部は、個人ごとの情報開示手続の一部として、各個人により指定された、該各個人本人であることを認証する認証手続が登録されたものであって、

前記開示手続実行部は、該特定の個人の前記開示依頼通知部により情報開示の承認を受けた後において、前記開示手続格納部に格納された前記特定の個人の認証手続に合致した認証手続で該特定の個人の認証を行なう認証部を備えたものであることを特徴とする請求項 1 記載の個人情報管理装置。

【請求項 7】 前記開示手続格納部は、個人ごとに、該個人に代わって情報開示手続を進める権限が委譲された権限委譲者の登録が自在なものであって、

前記開示手続実行部は、特定の個人の情報の開示依頼を受け、前記開示手続格納部に該特定の個人に代わって情報開示手続を進める権限が委譲された権限委譲

者が登録されていた場合には、該特定の個人の情報を開示するための手続として、該開示手続格納部に格納された該権限委譲者の情報開示手続に合致した情報開示手続を実行するものであることを特徴とする請求項 1 記載の個人情報管理装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、通信回線網に接続された、個人情報を管理する個人情報管理装置に関する。

【0002】

【従来の技術】

近年、パーソナルコンピュータどうしを接続するインターネットの利用率が急進しており、例えば医療現場においても、電子カルテシステムの運用にデータセンタが利用されインターネットを通じてアクセスされるなど、様々な分野において情報管理システムそのものが変わってきている。

【0003】

【発明が解決しようとする課題】

このように急速に変化しつつある社会環境下において、例えば上記の電子カルテシステムにおける個人のカルテ情報などの個人情報がインターネットを介して不用意に開示あるいは公開されてしまうことを防止し、個人に不測の不利益を及ぼしかねない状況を生じさせないシステムを構築することが急務となってきている。

【0004】

本発明は、上記事情に鑑み、個人情報の保護が図られた個人情報管理装置を提供することを目的とする。

【0005】

【課題を解決するための手段】

上記目的を達成する本発明の個人情報管理装置は、通信回線網に接続された、個人情報を管理する個人情報管理装置であって、

個人ごとの情報が登録された個人情報格納部と、

各個人により指定された各個人ごとの情報開示手続が登録された開示手続格納部と、

通信回線網を経由した、特定の個人の情報の開示依頼を受け、開示手続格納部に格納された、その特定の個人の情報開示手続に合致した情報開示手続を実行し、その情報開示手続が満足された場合にその特定の個人の情報を依頼元に向けて通信回線網に送信する開示手続実行部とを備えたことを特徴とする。

【 0 0 0 6 】

本発明の個人情報管理装置は、各個人により指定された、各個人ごとの情報開示手続を格納しておいて、ある特定の個人の情報開示にあたっては、その特定の個人によりあらかじめ指定されている情報開示手続に従って情報開示を行なうものであり、その個人の意に反した情報開示は防止され、したがってその個人が不測の不利益を被ることが防止される。

【 0 0 0 7 】

ここで、上記本発明の個人情報管理装置において、上記個人情報格納部は、個人ごとの情報の中の各個別の情報それぞれがその各個人により複数のランクのうちいずれかのランクに指定されることにより、各個人内で複数にランク付けされてなる個人情報が登録されたものであり、

上記開示手続格納部は、各個人により指定された、各個人内の各ランクに応じた情報開示手続が登録されたものであって、

上記開示手続実行部は、特定の個人の情報の開示依頼を受け、上記開示手続格納部に格納された、その特定の個人の、開示依頼を受けた情報のランクに応じた情報開示手続に合致した情報開示手続を実行するものであることが好ましい。

【 0 0 0 8 】

個人情報の中には、開示されてもさしたる支障のない個人情報や、J I S Q 1 5 0 0 1 に規定されている、人種、民族、精神障害、信教等々の、極秘にされるべき機微の個人情報など、情報開示に関し様々なレベルの個人情報が存在する。

【 0 0 0 9 】

そこで、上記のように、各個人内で個人情報を複数のランクに分けておき、個人情報の開示にあたっては、開示しようとするように応じた情報開示手続に従って開示することにより、一層きめ細かに、個人情報の保護と開示のバランスをとることができる。

【 0 0 1 0 】

ここで、各ランクごとの情報開示手続は、各個人により各個人ごとに指定されたものであり、どのランクの情報であってもその個人の意図に反して開示されることが防止される。また、ここでは、各個別の個人情報のランクの指定も各個人に委ねられているため、各個別の個人情報についても各個人の考え方や環境に応じた保護が図られる。

【 0 0 1 1 】

また、上記本発明の個人情報管理装置において、上記開示手続格納部は、各個人により指定された、各個人ごとの平常時の情報開示手続に加え、各個人により指定された、各個人ごとの緊急時の情報開示手続が登録されたものであって、

上記開示手続実行部は、平常時と緊急時とを識別する情報を伴った、特定の個人の情報の開示依頼を受け、その開示依頼が平常時あるいは緊急時のいずれに属するかに応じて、開示手続格納部に格納された、その特定の個人の、それぞれ平常時の情報開示手続あるいは緊急時の情報開示手続に合致した情報開示手続を実行するものであることが好ましい。

【 0 0 1 2 】

緊急時、例えば本人が事故に遭遇して情報開示の意図を伝えることができないような状況においてまで平常時と同一の情報開示手続を要求するのは適当ではなく、平常時と緊急時とを分け、緊急時には、あらかじめ各個人により指定された、各個人の緊急時の情報開示手続に従うことが好ましいからである。

【 0 0 1 3 】

また、上記本発明の個人情報管理装置において、上記開示手続格納部は、個人ごとの情報開示手続の一部として、各個人により指定された、その個人への連絡手続が登録されたものであって、

上記開示手続実行部は、特定の個人の情報の開示依頼を受けて、その特定の個

人に、上記開示手続格納部に格納されたその特定の個人への連絡手続に合致した連絡手続で、個人情報の開示依頼があった旨通知して、通知を受けた個人からの情報開示の承認を受ける開示依頼通知部を備え、その開示依頼通知部により情報開示の承認を受けて、さらに情報開示手続を進めるものであることが好ましい。

【 0 0 1 4 】

ある個人の情報の開示依頼があった場合に、情報開示手続の一部に、その個人に連絡してその個人の情報の開示依頼があったことを通知し、情報開示について、その個人の承諾を受けるという手続を含ませることにより、その個人が知らない間に自分の情報が開示されるという事態を避けることができる。

【 0 0 1 5 】

さらに、上記本発明の個人情報管理装置において、上記開示手続格納部は、個人ごとの情報開示手続の一部として、各個人により指定された、その個人本人であることを認証する認証手続が登録されたものであって、

上記開示手続実行部は、特定の個人の情報の開示依頼を受けて、上記開示手続格納部に格納されたその特定の個人の認証手続に合致した認証手続でその特定の個人の認証を行なう認証部を備えたものであることが好ましい。

【 0 0 1 6 】

個人情報を開示する場合、その個人の許可を得るとともに、認定手続により、その許可した本人が正にその本人であることを確認することが好ましいが、その認証手続も、その個人があらかじめ指定しておいた認証手続に沿って進めることによりその個人の意思を反映させることができる。

【 0 0 1 7 】

ここで、上記のような、開示依頼通知部と認証部との双方を備えた場合、上記開示手続実行部は、開示依頼通知部により情報開示の承認を受けた後において、認証部により、開示手続格納部に格納された特定の個人の認証手続に合致した認証手続でその特定の個人の認証を行なうが好ましい。

【 0 0 1 8 】

さらに、上記本発明の個人情報管理装置において、上記開示手続格納部は、個人ごとに、その個人に代わって情報開示手続を進める権限が委譲された権限委譲

者の登録が自在なものであって、

上記開示手続実行部は、特定の個人の情報の開示依頼を受け、開示手続格納部にその特定の個人に代わって情報開示手続を進める権限が委譲された権限委譲者が登録されていた場合には、その特定の個人の情報を開示するための手続として、開示手続格納部に格納された、その権限委譲者の情報開示手続に合致した情報開示手続を実行するものであることが好ましい。

【 0 0 1 9 】

こうすることにより、例えば子供に対する親権者や、要介護人に対する介護者等が、本人に代わって、その本人の個人情報を保護しつつ、その本人の個人情報の開示手続を進めることができる。

【 0 0 2 0 】

【発明の実施の形態】

以下、本発明の実施形態について説明する。

【 0 0 2 1 】

図 1 は、本発明の個人情報管理装置の一実施形態を含む個人情報管理・開示システムの一例を示す模式図である。

【 0 0 2 2 】

ここには、本発明の個人情報管理装置の一実施形態に相当する 1 台のサーバマシン 1 0 0 と、代表的に 2 台のクライアントマシン 2 0 0, 3 0 0 が示されており、それらは通信回線網 5 0 0 に接続されている。

【 0 0 2 3 】

2 台のクライアントマシン 2 0 0, 3 0 0 のうちの 1 台のクライアントマシン 2 0 0 は、情報提供者側のクライアントマシンであり、もう 1 台のクライアントマシン 3 0 0 は、情報利用者側のクライアントマシンである。ここには情報提供者側のクライアントマシンと情報利用者側のクライアントマシンが 1 台ずつ示されているが、これらは代表的に示したものであり、通常は、多数台の情報提供者側のクライアントマシンおよび多数台の情報利用者側のクライアントマシンが通信回線網 5 0 0 に接続されている。

【 0 0 2 4 】

情報提供者側のクライアントマシン200には、携帯電話210が接続されている。すなわち、例えば、クライアントマシン200に送られてきた電子メールが携帯電話210に転送されたり、また、携帯電話210はクライアントマシン200を介してこのシステムにアクセス可能となっている。この図1では、携帯電話210は、矢印により、クライアントマシン200に直接に接続されているかのように示されているが、この矢印はクライアントマシン200と携帯電話210が上記の意味で接続されていることのみを示すものであって、実際には、それらは、図示しない無線通信回線を含む通信回線網500を介して接続されている。

【0025】

この図1に示すサーバマシン100および2台のクライアントマシン200, 300は、CPU、主記憶装置、ハードディスク、通信用ボード等が内蔵された本体部101, 201, 301、本体部101, 201, 301からの指示により表示画面102a, 202a, 302a上に画像や文字列を表示する表示部102, 202, 302、サーバマシン100および各クライアントマシン200, 300にユーザの指示を入力するためのキーボード103, 203, 303、表示画面102a, 202a, 302a上の任意の位置を指定することにより、その指定時にその位置に表示されていたアイコン等に応じた指示を入力するマウス104, 204, 304を備えている。

【0026】

また、サーバマシン100およびクライアントマシン200, 300の本体部101, 201, 301にはさらに、外観上、フロッピーディスク(FD)、CDROM(図1には図示せず:図2参照)が装填されるFD装填口101a, 201a, 301a、CDROM装填口101b, 201b, 301bを有しており、それらの内部には、それらの装填口101a, 201a, 301a; 101b, 201b, 301bから装填されたフロッピーディスクやCDROMをドライブしてアクセスする、フロッピーディスクドライブ、CDROMドライブも内蔵されている。さらに、これらサーバマシン100および各クライアントマシン200, 300の本体部101, 201, 301は、通信回線網500に接続さ

れている。

【 0 0 2 7 】

さらに各クライアントマシン 2 0 0, 3 0 0 には、音声を入力するためのマイクロホン 2 0 5, 3 0 5、および指紋を読み取る指紋読取装置 2 0 6, 3 0 6 が接続されている。

【 0 0 2 8 】

さらに、上述したように、情報提供者側のクライアントマシン 2 0 0 には携帯電話 2 1 0 が接続されている。

【 0 0 2 9 】

図 2 は、図 1 に示すサーバマシンのハードウェア構成図である。クライアントマシンについては、マイクロホンと指紋読取装置が接続されていることを除き、サーバマシンと同様なハードウェア構成を有しており、ここでは、サーバマシンのハードウェア構成の図示および説明で代表させる。

【 0 0 3 0 】

ここには、中央演算処理装置 (CPU) 1 1 1、RAM 1 1 2、ハードディスクコントローラ 1 1 3、FD ドライブ 1 1 4、CDROM ドライブ 1 1 5、マウスコントローラ 1 1 6、キーボードコントローラ 1 1 7、ディスプレイコントローラ 1 1 8、および通信用ボード 1 1 9 が備えられており、それらはバス 1 1 0 で相互に接続されている。

【 0 0 3 1 】

FD ドライブ 1 1 4、CDROM ドライブ 1 1 5 は、図 1 を参照して説明したように、フロッピーディスク 6 1 0、CDROM 6 2 0 が装填され、装填されたフロッピーディスク 6 1 0、CDROM 6 2 0 をアクセスするものである。

【 0 0 3 2 】

また、ここには、ハードディスクコントローラ 1 1 3 によりアクセスされるハードディスク 1 2 0、マウスコントローラ 1 1 6 により制御されるマウス 1 0 4、キーボードコントローラ 1 1 7 により制御されるキーボード 1 0 3、ディスプレイコントローラ 1 1 8 により制御される表示部 1 0 2、および通信用ボード 1 1 9 を介して接続される通信回線網 5 0 0 も示されている。

【 0 0 3 3 】

CDROM620には、図1に示すサーバマシン100を、本発明の個人情報管理装置の一実施形態として動作させるための個人情報管理プログラムが記憶されており、CDROMドライブ115により、そのCDROM620から個人情報管理プログラムが読み込まれ、バス110を経由し、ハードディスクコントローラ113によりハードディスク120内に格納される。実際の実行にあたっては、そのハードディスク120内の個人情報管理プログラムはRAM112上にロードされ、CPU111により実行される。

【 0 0 3 4 】

図3は、本発明の個人情報管理装置の一実施形態を表わす機能ブロック図である。この図3に示す個人情報管理装置は、図1、図2に示すサーバマシン100のハードウェアと、CDROM620からインストールされた個人情報管理プログラムとの複合、及びその後の個人情報等の蓄積により構成されたものである。

【 0 0 3 5 】

この図3に示す個人情報管理装置700は、個人情報格納部710と、開示手続格納部720と、開示手続実行部730とから構成され、開示手続実行部730は、さらに開示依頼通知部731と認証部732を備えている。

【 0 0 3 6 】

個人情報格納部710には、個人ごとの情報が登録されている。

【 0 0 3 7 】

図4は、個人情報格納部に登録された個人情報テーブルを示す図である。

【 0 0 3 8 】

ここには、1人分の個人情報の極く一部が示されており、そこには、住民基本番号、住所、氏名、生年月日、性別、介護等級、……等々、様々な個人情報が列記されている。

【 0 0 3 9 】

図3の開示手続格納部720には、各個人により指定された各個人ごとの情報開示手続が登録されている。

【 0 0 4 0 】

図5～図10は、各個人ごとの情報開示手続を実行するのに必要な各種テーブルの例を示す図である。

【0041】

具体的には図5，図6，……，図10には、それぞれ、認証用データテーブル、情報開示手続テーブル、平常時認証テーブル、緊急時認証テーブル、通信順テーブル、および権限委譲テーブルが示されている。

【0042】

図5に示す認証用データテーブルは、各個人について1つずつ作成されている。この認証用データテーブルには、その個人の認証に必要となる、例えばパスワード、指紋、声紋、DNA、……等々のデータが登録されている。尚、この認証用データテーブルは個人情報的一种でもあり、これらのデータは、図4の個人情報テーブルに含まれていてもよいが、ここでは後の説明の都合上、個人情報テーブルとは別に認証用データテーブルを置いている。

【0043】

また、図6に示す情報開示手続テーブルは、各個人の各開示レベルそれぞれについて1つずつ作成されている。この情報開示手続テーブルには、開示レベル、開示項目、および認証方法が登録されている。開示レベルは、本実施形態では、1～5のランクに分けられており、その数値が大きくなるほど秘密性が高いことを意味している。開示項目の欄には、その開示レベル（この図6に示す例では開示レベル1）に相当する個人情報の項目が列挙されている。また、認証方法の欄には、その開示レベルの個人情報を開示するための認証方法が登録されている。ただし、ここには、直接的には、その認証方法が登録された、図7の平常時認証テーブルを指し示すポインタが登録されている。

【0044】

この図6に示す情報開示手続テーブルは、標準的な構成のガイダンスを受けつつも、その個人の考えで登録されたものである。すなわち、例えば開示レベル1に、どの個人情報を登録するか、あるいは、開示レベル1の個人情報を開示するための認証方法をどうするかは、その個人の判断に委ねられている。

【0045】

図7に示す平常時認証テーブルは、図6の情報開示手続テーブルと同様、各個人の各開示レベルごとに作成されており、それぞれが各個人の各開示レベルごとの情報開示手続テーブル（図6参照）の認証方法の欄のポインタで指し示されている。各開示レベルごとの平常時認証テーブルには、その個人の、平常時の、各開示レベルごとの認証手続が登録されている。

【0046】

この図7に示す例では、平常時には、パスワードと、指紋と、声紋の全てが一致した場合のみ、そのリンクされた情報開示手続テーブル（図6参照）に項目が列挙されている個人情報の開示を許可することを意味している。

【0047】

図8に示す緊急時認証テーブルは、各個人につき1つずつ作成されており、そこには、その個人が意識不明に陥ったときなど、その個人が情報開示／非開示の意思をあらわすことができず、かつ、その個人の情報が緊急に必要な場合の認証方法が登録されている。この図8に示す例では、緊急時には、その個人の指紋あるいはDNAのいずれか1つが確認されることをもって、その個人の情報を開示することを示している。この図8の緊急時認証テーブルも、その個人の意思で登録されており、仮に、この緊急時認証テーブルが空欄であった場合、あるいは本人自身でないと認証が不可能な、例えばパスワードのみが登録されていた場合は、法律上規定された例外等の場合を除き、たとえその個人の生命が危機に晒された場合であっても情報は開示されない。緊急時の情報開示の依頼は、もともと救急指定病院の医師等、限られた者にのみ許可されており、本実施形態では、この緊急時認証テーブルに登録された認証方法に合致した場合、依頼に応じて全ての情報が開示される。ただし、緊急時であっても、例えば犯罪歴、門地等、緊急性に乏しくかつ秘密性の高い情報は非開示とするなど、開示される情報に制限を加えてもよい。

【0048】

図9に示す通知順テーブルは、各個人ごとに作成されており、そこには、その個人に何かを通知するときの通知方法の順序が登録されている。この通知順テーブルも各個人が自分の意思で登録する。図9に示す例は、先ずは携帯電話に連絡

し、通じなかったときはそこに登録された別の電話にかけ、それでも通じなかったときは電子メールで連絡し、所定時間（例えば15分間）経過しても返答がないときは代理人1に連絡をし、代理人1への連絡を試みても連絡できないときは代理人2に連絡することを意味している。代理人1、代理人2への連絡方法は、図9に示す通知順テーブルと同様な、その代理人1、代理人2の通知順テーブルに従うことになる。ただし、その代理人個人の通知順テーブルに、その代理人個人の、さらなる代理人が登録されていても、代理人個人の代理人への連絡は行なわれない。

【0049】

図10に示す権限委譲テーブルは、各個人のうちの必要な個人について作成される。

【0050】

例えば、その個人が所定年齢以下の子供のときは、この権限委譲テーブルにはその子供の親権者が登録され、あるいは、その個人が要介護者であって介護等級が所定等級以上のときは、その要介護者を介護する介護人が登録される。

【0051】

図3に戻って説明を続ける。

【0052】

開示手続実行部730は、基本的には、通信回線網500を経由した、特定の個人の情報の開示依頼を受け、開示手続格納部720に格納された、その特定の個人の情報開示手続に合致した情報開示手続を実行し、その情報開示手続が満足された場合に、個人情報格納部710に格納された個人情報の中から、その特定の個人の開示要求を受けた情報を抽出し、その抽出した情報を依頼元に向けて通信回線網500に送信するものである。具体的には、開示手続格納部720に、個人ごとの情報開示手続の一部として、各個人により指定されたその個人への連絡手続と、各個人により指定されたその個人本人であることを認証する認証手続が登録されており、開示手続実行部730は、特定の個人の情報の開示依頼を受けて、基本的には先ず開示依頼通知部731により、その特定の個人に、開示手続格納部720に格納されたその特定の個人への連絡手続に合致した連絡手続で

、個人情報の開示依頼があった旨通知して、通知を受けた個人からの情報開示の承認を受ける。次に、開示手続実行部 7 3 0 は、今度は認証部 7 3 2 により、開示手続格納部 7 2 0 に格納されたその特定の個人の認証手続に合致した認証手続でその特定の個人の認証を行なう。ただし、その特定の個人本人ではなく、その代理人や保護者等に連絡し、その代理人や保護者等の認証を行なう場合もある。詳細は後述する。この認証手続が正しく終了すると、開示要求を受けた情報が抽出され要求元に向けて送信される。

【 0 0 5 3 】

以下、個人情報開示の手続きの一例について説明するが、ここでは、その説明のための 1 つの場面設定として、図 1 に示すクライアントマシン 2 0 0 を自宅に備えた患者が、携帯電話 2 1 0 を持って、診察のために、クライアントマシン 3 0 0 が設置された医院を訪れた場面を想定する。

【 0 0 5 4 】

図 1 1 は、図 2 に示すサーバマシン 1 0 0 における情報開示手続を示すフローチャートである。

【 0 0 5 5 】

図 1 のクライアントマシン 3 0 0 が設置された医院の医師は、訪れてきた患者の病歴やアレルギー体質等を知るために、クライアントマシン 3 0 0 を操作して、サーバマシン 1 0 0 に対して、その患者のそれらに関する情報を送るよう要求する。

【 0 0 5 6 】

サーバマシン 1 0 0 は、情報開示要求を受信すると（図 1 1 ステップ S 1 ）、その情報開示要求が、この実施形態の対象である個人情報の開示要求であるか否かを判断し（ステップ S 2 ）、個人情報とは無関係の情報開示要求（例えば政府や公共機関の案内など）であったときは、その情報の性質に合った処理がなされる（ステップ S 3 ）。

【 0 0 5 7 】

ステップ S 2 で、今回の情報開示要求が個人情報の開示要求である旨判定されると、次にその開示要求が緊急のものか否かが判定される。

【0058】

ステップS4で平常時の情報開示要求である旨判定されると、ステップS5に進み、その個人情報の持ち主、すなわちここでは、医院を訪れた患者に向けて個人情報の開示要求があった旨通知され、その個人（患者）の、個人情報開示の同意が求められる。その開示に同意が得られないときは、非開示となり（ステップS6）、その旨開示要求元に通知される。ステップS5の詳細については後述する。

【0059】

開示に対し同意があったときはステップS7に進み、平常時の認証手続きが行なわれる。この平常時認証手続きの詳細についても後述する。

【0060】

また、ステップS4で緊急である旨判定されると緊急時の認証手続きが行なわれる（ステップS8）。この緊急時認証手続きについても後述する。

【0061】

ステップS7あるいはステップS8の認証手続きで正しく認証が行なわれると（ステップS9）、その個人（患者）の、要求された個人情報が、その要求元（クライアントマシン300）に対し開示される（ステップS10）。一方、認証に失敗すると非開示となり（ステップS6）、要求元に対しその旨通知される。

【0062】

図12は、図11のステップS5に示す、個人情報開示要求通知および開示の同意を求める手順の詳細フローを示す図である。

【0063】

ここではまず、情報開示要求を受けた情報の所有者である個人が他の個人の保護下にあるか否かが判定される（ステップS51）。

【0064】

ここでは、例えば情報開示要求を受けた情報の所有者である個人（患者）の個人情報テーブル（図4参照）が参照され、その個人（患者）が所定年齢以下の子供であったり、あるいは介護等級が高い重度障害者であったりしたときは、その個人の情報開示の責任はその個人の保護者等にあり、そのときは、その個人の権

限委譲テーブル（図 1 0 参照）が参照されて、その個人の情報開示の権限の委譲を受けている保護者等に対し、その個人の情報の開示要求があった旨通知される（ステップ S 5 7）。

【 0 0 6 5 】

そのような保護を必要としない通常の大人の場合は、その本人に対し、情報開示要求があった旨通知される（ステップ S 5 2）。このときの本人への通知にあたっては、その本人の通知順テーブルが参照され、この図 9 に示す例では、まず携帯電話に情報開示要求があった旨通知される。携帯電話からの応答がないときは、前述のとおり、その通知順テーブルにしたがって次の手順による通知が試みられる。

【 0 0 6 6 】

ここでは、その通知を受ける個人である患者は自分の携帯電話を持参して医院を訪れており、自分の携帯電話が鳴り、自動音声により情報開示要求があった旨通知される。そこで、その携帯電話のボタン操作、あるいは声による応答により、その情報開示に対する同意、不同意の意思表示が行なわれる。

【 0 0 6 7 】

ここで、サーバマシン 1 0 0（図 1 参照）は、その本人から同意する旨通知を受けると、次のステップ S 7（図 1 1 参照）の平常時認証手続きに進み、一方、同意しない旨通知を受けると、ステップ S 6（図 1 1 参照）に進み、開示しない旨クライアントマシン 3 0 0 に通知される。

【 0 0 6 8 】

仮に、図 9 に示す通知順テーブルに従って、携帯電話、別の電話、電子メールの順に本人への連絡を試みても応答がなかったときは、ステップ S 5 4 に進み、その通知順テーブルに代理人が登録されているか否かが判定され、代理人が登録されているときは、その代理人への通知が試みられる（ステップ S 5 5）。代理人への通知は、その代理人によって登録される通知順テーブルに従って行なわれるが、前述したように、その代理人の通知順テーブルにその代理人の代理人が登録されていても、その代理人の代理人への通知は行なわれない。

【 0 0 6 9 】

本人の代理人への通知が試みられた結果、その代理人から情報開示許可の連絡が来たときはステップ S 7 に進み、このときはその情報開示許可を行なった代理人に対する認証手続きが行なわれる。代理人から情報開示不許可の回答が来たとき、あるいは代理人から（複数の代理人がいるときはそれら複数の代理人のいずれからでも）回答がなかったときは、ステップ S 6 に進み、非開示となる。

【 0 0 7 0 】

ステップ S 5 1 でその個人が他の個人の保護下にある旨判定されてステップ S 5 7 に進むと、その個人を保護する立場にある保護者等に対して、その保護者等の通知順テーブルに従って通知が試みられる。このとき、その保護者等の通知順テーブルに代理人が登録されていても、その代理人への連絡は行なわれない。

【 0 0 7 1 】

その保護者等に通知した結果（ステップ S 5 7）、その保護者等から情報開示許可の回答を受けたときはステップ S 7 に進み、このときは、その保護者等に対して平常時認証手続きが行なわれる。一方、その保護者等から開示不許可の回答を受けたとき、あるいはその保護者等から応答がなかったときは、ステップ S 6 に進み、非開示となる。

【 0 0 7 2 】

図 1 3 は、図 1 1 のステップ S 7 における平常時認証手続きの詳細フローを示す図である。

【 0 0 7 3 】

ここでは、その情報開示要求を受けた本人（患者）の情報開示テーブル（図 6 参照）が参照され、開示要求を受けた情報がどの開示レベルに指定されているか確認される（ステップ S 7 1）。

【 0 0 7 4 】

次いで、その個人（患者）の、その開示レベルに応じた平常時認証テーブル（図 7 参照）が参照される。ここで、その個人に代わり、代理人あるいは保護者等の認証手続きを行なうときは、その開示レベルに応じた、その代理人あるいは保護者等の平常時認証テーブルが参照される。ここでは、その個人本人の認証手続きを行なうものとして説明を続ける。

【 0 0 7 5 】

図 7 に示す例では、「パスワード」と「指紋」と「声紋」とにより認証を行なうことが登録されており、この場合、サーバマシン 1 0 0 は、クライアントマシン 3 0 0 に対して、そこに登録されているパスワード、指紋、声紋の入力を要求する。その医院を訪れている患者は、クライアントマシン 3 0 0 のキーボードから自分のパスワードを入力し、かつ指紋読取装置 3 6 0 に自分の指を押し当てて指紋を読み取らせ、さらにマイクロホン 3 0 5 に向かって発声することにより声紋を入力する。すると、それらのパスワード、指紋、声紋は、図 1 のサーバマシン 1 0 0 に送られ、サーバマシン 1 0 0 では、その送られて来たパスワード、指紋、声紋を、その個人（患者）の認証用データテーブル（図 5 参照）に登録されているパスワード、指紋、声紋と比較し、一致するか否かが判定される。

【 0 0 7 6 】

クライアントマシン 3 0 0 から送られて来たパスワード、指紋、声紋のすべてが本人のものであると判定されると、認証 OK となり、いずれか 1 つでも本人のものではない、あるいは、不明である旨判定されると認証 NG となる。図 1 1 のステップ S 9 では、その認証が OK か NG かが判定される。

【 0 0 7 7 】

図 1 4 は、図 1 1 の開示のステップ（ステップ S 1 0）の詳細フローを示す図である。

【 0 0 7 8 】

ここでは、その個人（患者）の個人情報テーブル（図 4 参照）が参照されて、開示要求のあった情報が抽出される（ステップ S 1 0 1）。また、本実施形態では、開示要求のなかったいくつかの情報について、偽情報を発生させて、その個人情報テーブルから抽出された情報に付加される（ステップ S 1 0 2）。このようにして一部に偽情報を含む個人情報が、その要求元であるクライアントマシン 3 0 0 に送信される（ステップ S 1 0 3）。

【 0 0 7 9 】

クライアントマシン 3 0 0 は、自分がどの情報について開示要求を行なったか知っているため、受信した、偽情報を含む情報の中から正しい情報のみを抽出す

ることができる。この正しい情報と偽情報との区別をクライアントマシン300の操作を行なった医師等の人間に委ねると思わぬミスを生じるおそれがあるため、クライアントマシン300がどのような情報について開示要求を行なったかを記憶しておき、サーバマシン100から受け取った情報の中から開示を要求した情報のみを抽出し、正しい情報のみを医師等に提示することが好ましい。このように一部に偽情報を含ませることにより、サーバマシン100からクライアントマシン300に送信される途中で悪意の第三者がその個人情報を盗んでも正しい情報と偽りの情報とが識別できず、個人情報が保護されることになる。

【0080】

図11のステップS8の緊急時認証手続が行なわれる場合の例としては、例えば患者が意識不明で医院に運び込まれた場合を挙げることができる。

【0081】

その医院は救急医療を行なう医院としてあらかじめサーバマシン100に登録されており、その医院の設置されているクライアントマシン300に特別なパスワード等を入力して操作することにより、サーバマシン100では、そのクライアントマシン300からの情報開示要求が緊急性の高いものとして取り扱われる。

【0082】

ステップS8では、このような場合の認証手続が行なわれるが、ここでは、その本人（患者）の緊急時認証テーブル（図8参照）が参照される。

【0083】

この図8に示す例では、あらかじめその本人により指紋とDNAとのいずれかで認証を行なうことが登録されており、サーバマシン100は、クライアントマシン300に対し、指紋あるいはDNAのデータを送るよう要求する。クライアントマシン300では、その運び込まれた患者の指紋を指紋読取装置306で採取してサーバマシン100に送り、あるいは、例えば事故で指が切断されていて指紋が使えないときはDNA分析を行なってその結果をクライアントマシン300に入力しサーバマシン100に送信する。

【0084】

サーバマシン 100 では、その個人（患者）の認証用データテーブルを参照し、指紋が送られてきたときはその指紋が本人のものか否かが判定され、DNA の分析結果が送られてきたときはその DNA が本人のものか否かが判定される。この緊急時認証手続（ステップ S 8）では、その緊急時認証テーブル（図 8 参照）に格納されている項目のうちのいずれか 1 つでも本人のものと認定されると認証 OK となる。

【0085】

ステップ S 8 の緊急時認証手続で認証 OK あるいは認証 NG となった後の手続は、ステップ S 7 の平常時認証手続で認証 OK あるいは認証 NG となった後の手続と同様である。

【0086】

なお、以上の説明では省略したが、図 1 に示すシステムにおける、サーバマシン 100 と各クライアントマシン 200, 300 との間の通信は暗号化された形式で行なわれ、受信した側で復号化される。それら暗号化、復号化の技術としては既存の技術が用いられる。

【0087】

【発明の効果】

以上説明したように、本発明によれば、個人情報があるに保護されるとともに、その有効利用が図られる。

【図面の簡単な説明】

【図 1】

本発明の個人情報管理装置の一実施形態を含む個人情報管理・開示システムの一例を示す模式図である。

【図 2】

図 1 に示すサーバマシンのハードウェア構成図である。

【図 3】

本発明の個人情報管理装置の一実施形態を表わす機能ブロック図である。

【図 4】

個人情報格納部に登録された個人情報テーブルを示す図である。

【図 5】

認証用データテーブルの例を示す図である。

【図 6】

情報開示手続テーブルの例を示す図である。

【図 7】

平常時認証テーブルの例を示す図である。

【図 8】

緊急時認証テーブルの例を示す図である。

【図 9】

通知順テーブルの例を示す図である。

【図 1 0】

権限委譲テーブルの例を示す図である。

【図 1 1】

サーバマシンにおける情報開示手続を示すフローチャートである。

【図 1 2】

図 1 1 のステップ S 5 に示す、個人情報開示要求通知および開示の同意を求める手続の詳細フローを示す図である。

【図 1 3】

図 1 1 のステップ S 7 における平常時認証手続の詳細フローを示す図である。

【図 1 4】

図 1 1 の開示のステップ（ステップ S 1 0）の詳細フローを示す図である。

【符号の説明】

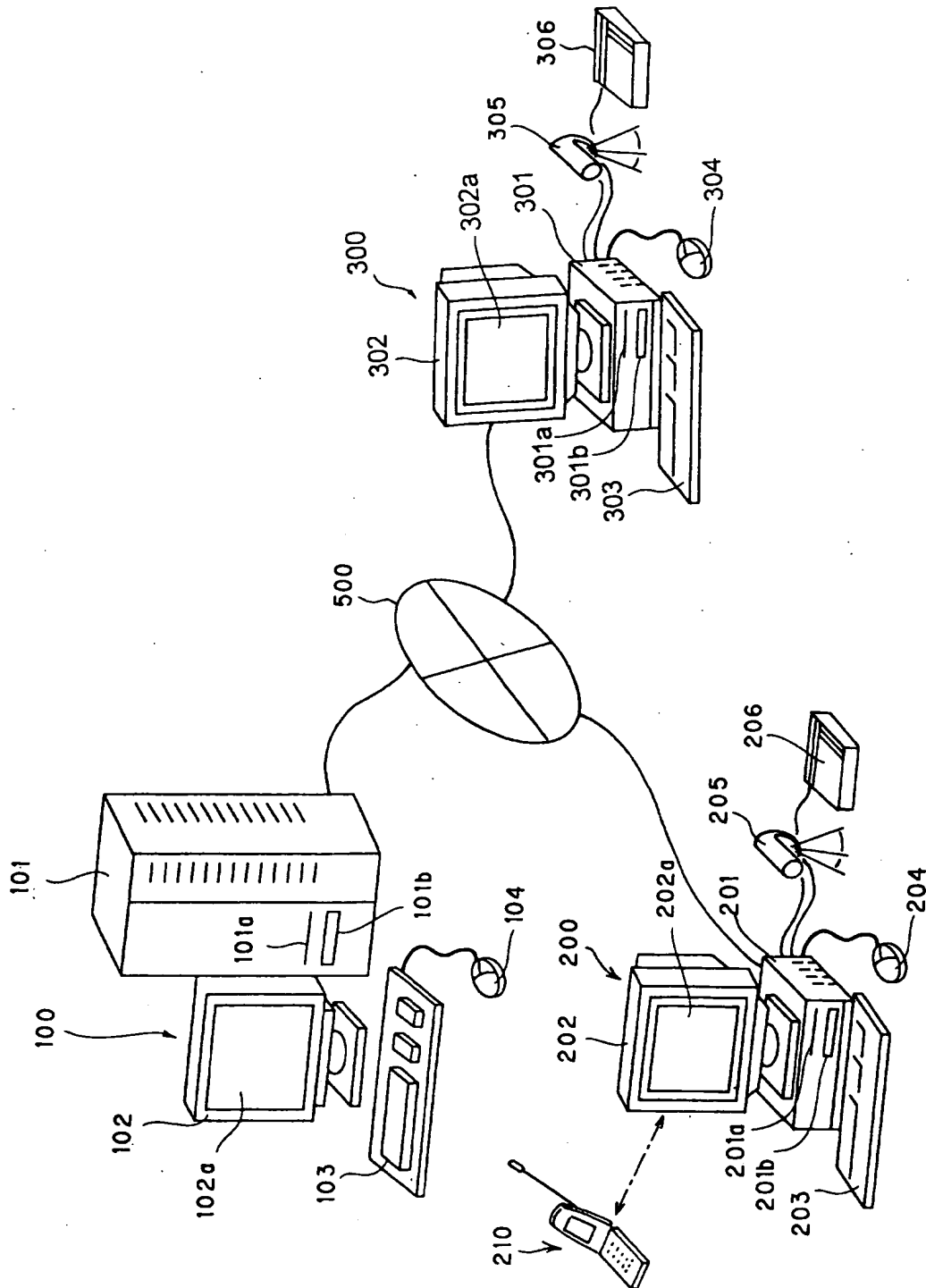
- 1 0 0 サーバマシン
- 2 0 0, 3 0 0 クライアントマシン
- 1 0 1, 2 0 1, 3 0 1 本体部
- 1 0 2, 2 0 2, 3 0 2 表示部
- 1 0 2 a, 2 0 2 a, 3 0 2 a 表示画面
- 1 0 3, 2 0 2, 3 0 3 キーボード
- 1 0 4, 2 0 4, 3 0 4 マウス

2 0 5, 3 0 5 マイクロホン
2 0 6, 3 0 6 指紋読取装置
2 1 0 携帯電話
5 0 0 通信回線網
7 0 0 個人情報管理装置
7 1 0 個人情報格納部
7 2 0 開示手続格納部
7 3 0 開示手続実行部
7 3 1 開示依頼通知部
7 3 2 認証部

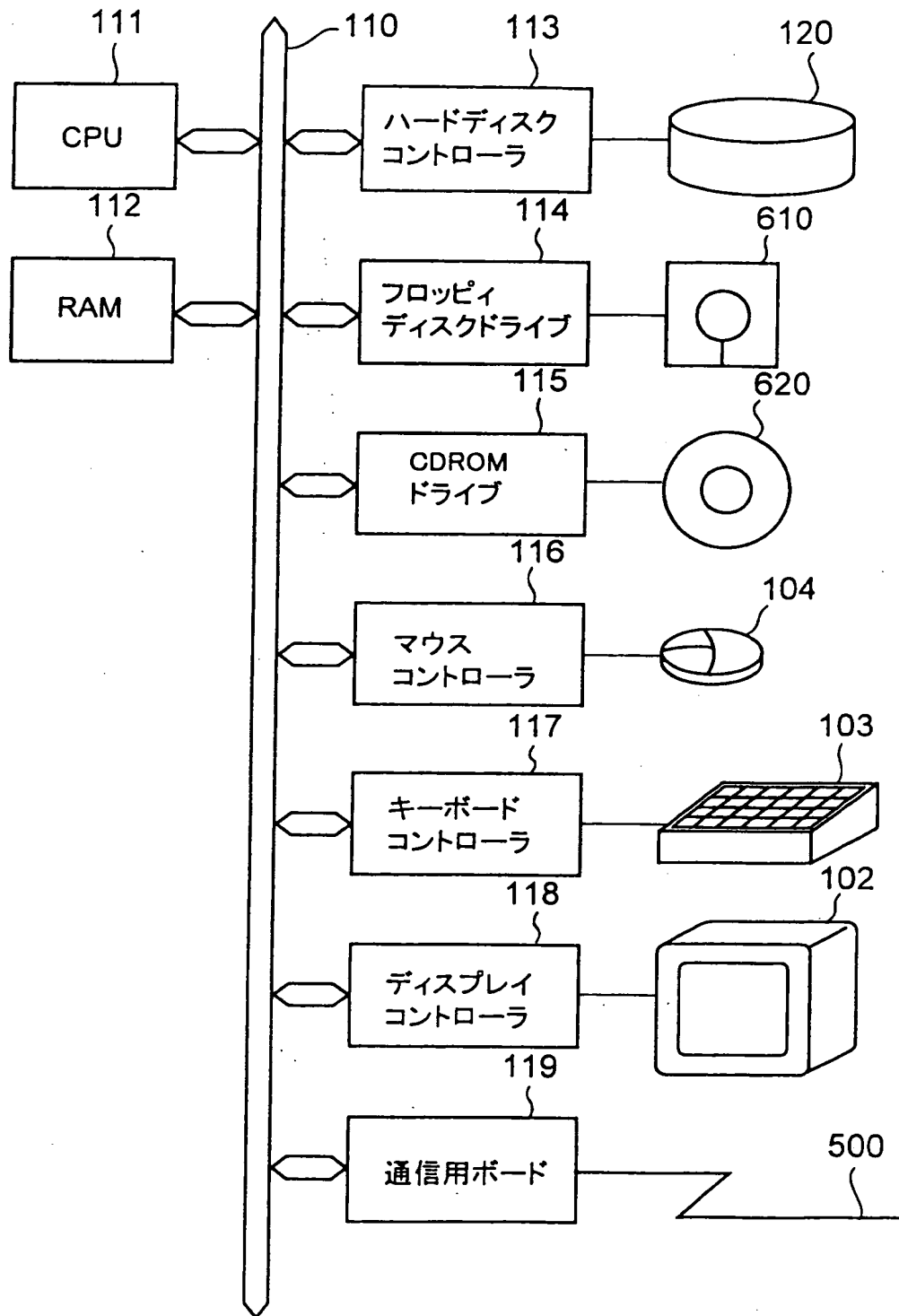
【書類名】

図面

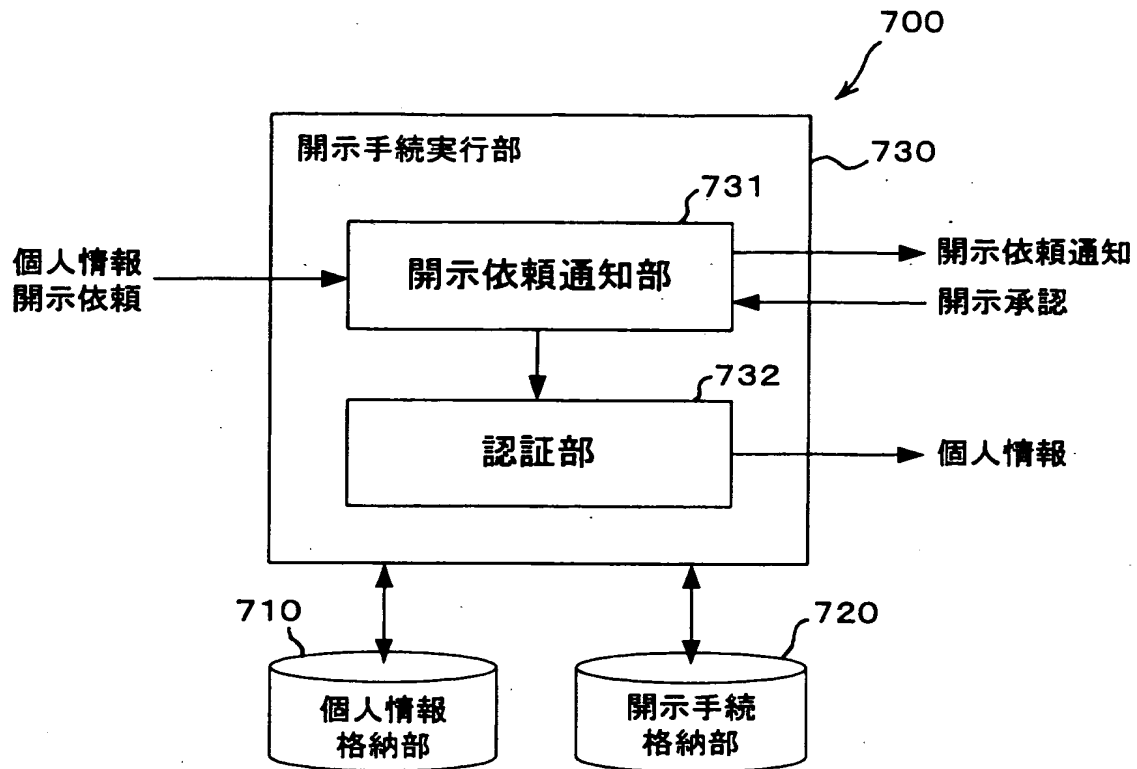
【図 1】



【図 2】



【図 3】



【図 4】

個人情報テーブル

住民基本番号	住所	氏名	生年月日	性別	介護等級	-----
--------	----	----	------	----	------	-------

【図 5】

認証用データテーブル

パスワード	指紋	声紋	DNA	-----
-------	----	----	-----	-------

【図 6】

情報開示手続テーブル

開示レベル	開示項目	認証方法
1	住所、氏名、-----	(ポインタ)

【図 7】

平常時認証テーブル

パスワード	指紋	声紋
-------	----	----

【図 8】

緊急時認証テーブル

指紋	DNA
----	-----

【図 9】

通知順テーブル

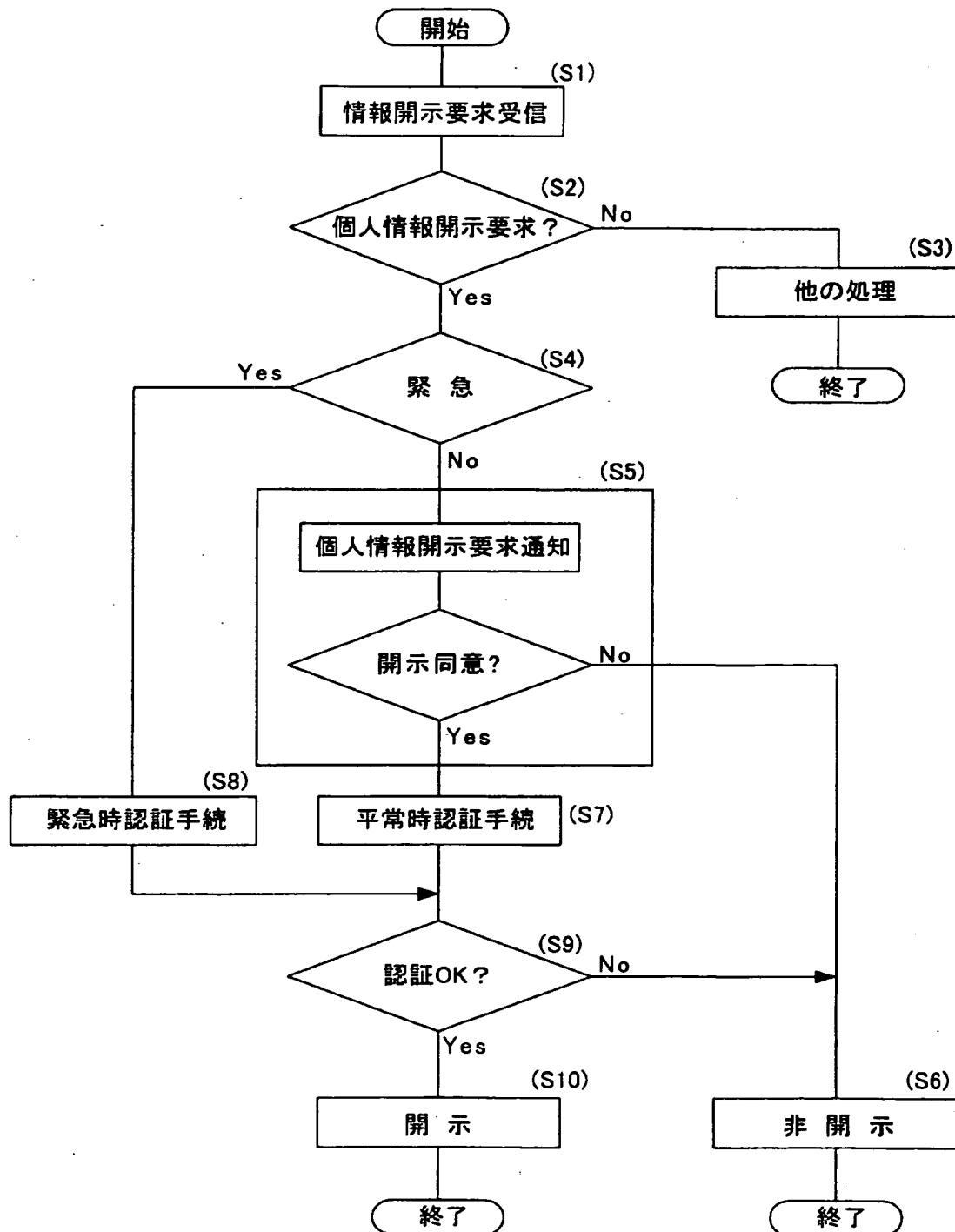
携帯	電話	メール	代理人1	代理人2	-----
----	----	-----	------	------	-------

【図 10】

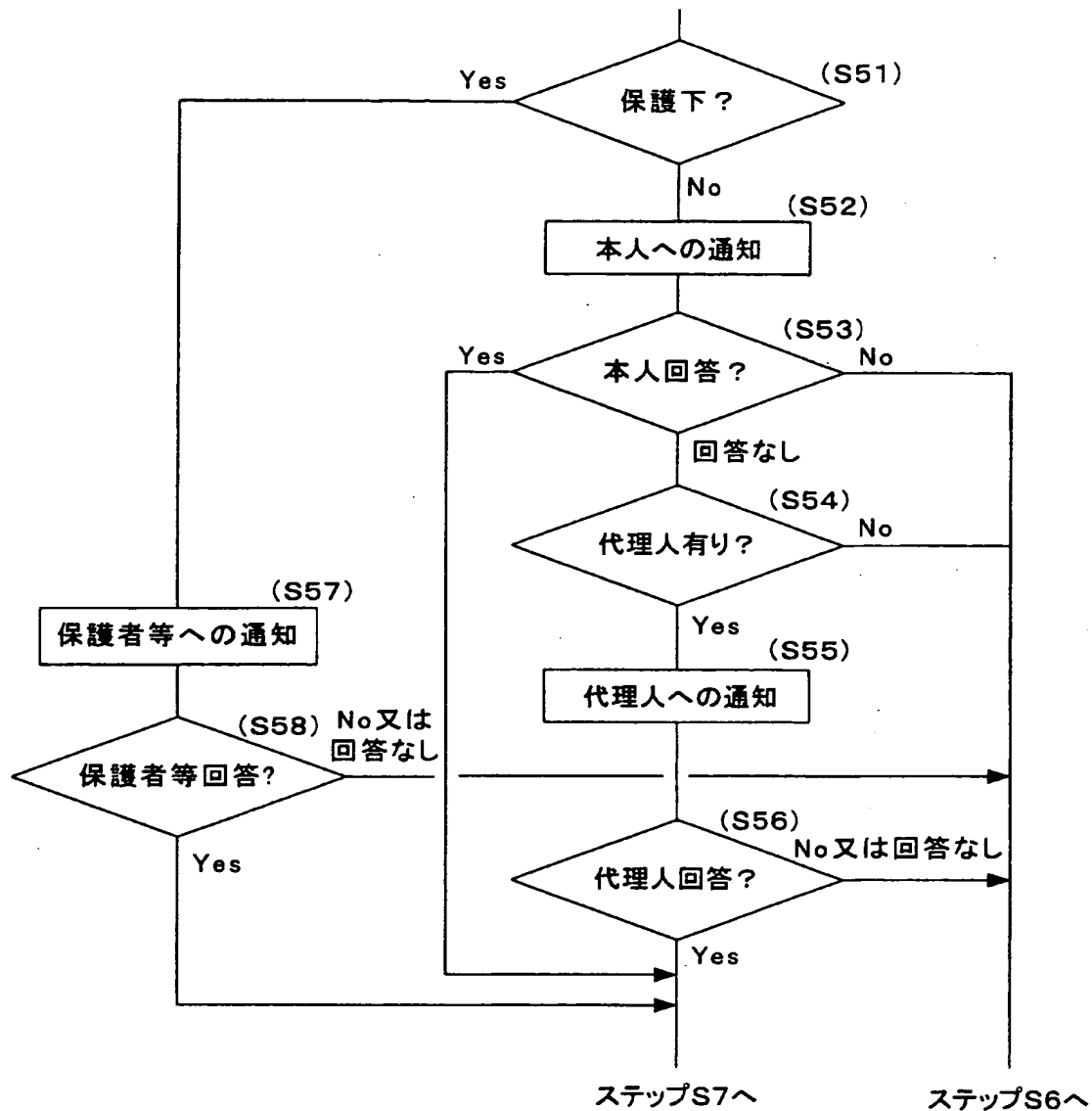
権限委譲テーブル

保護者	介護者	-----
-----	-----	-------

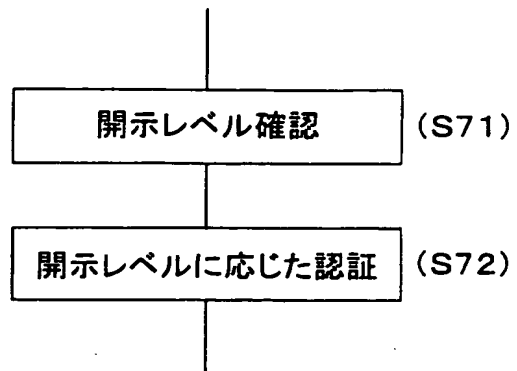
【図 11】



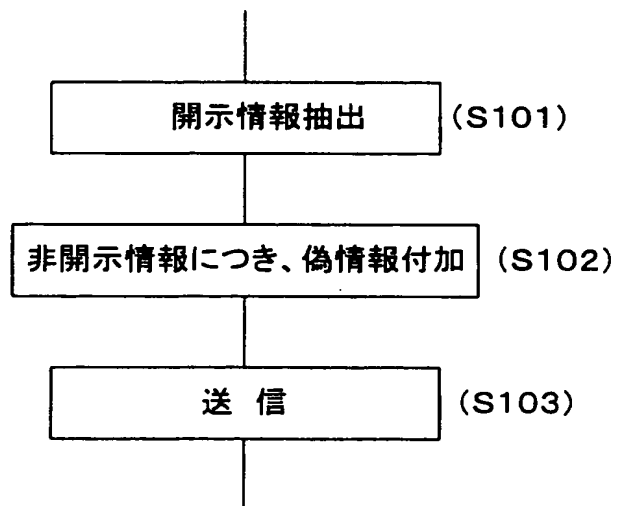
【図 12】



【図13】



【図14】



【書類名】 要約書

【要約】

【課題】 本発明は、通信回線網に接続された、個人情報を管理する個人情報管理装置に関し、個人情報を有効に保護する。

【解決手段】 個人ごとの情報が登録された個人情報格納部と、各個人により指定された各個人ごとの情報開示手続が登録されてなる開示手続格納部とを保護するとともに、特定の個人の情報の開示依頼を受けて、該特定の個人に、前記開示手続格納部に格納された該特定の個人への連絡手続に合致した連絡手続で、個人情報の開示依頼があった旨連絡して、連絡を受けた個人からの情報開示の承認を受ける開示依頼通知部と、前記開示手続格納部に格納された前記特定の個人の認証手続に合致した認証手続で該特定の個人の認証を行なう認証部とを有する開示手段実行部 7 3 0 を備えた。

【選択図】 図 3

出 願 人 履 歴 情 報

識別番号 [000005223]

1. 変更年月日	1996年 3月26日
[変更理由]	住所変更
住 所	神奈川県川崎市中原区上小田中4丁目1番1号
氏 名	富士通株式会社